ТЕОРИЯ ЧИСЕЛ

асс. А. В. Устинов

1/2 года, 4 курс, экономический поток

1. Алгоритм Евклида и его сложность. Теорема Ламе. Расширенный алгоритм Евклида. ([1], 2.2., [3], 4.3., [2], 3, [4], 1.)

2. Конечные непрерывные дроби. Свойства подходящих дробей. ([1], 2.2., [2], 5, [4], 1.)

3. Бесконечные непрерывные дроби. Однозначность представления действительных чисел непрерывными дробями. Теорема Лагранжа. ([2], 24, 28.)

4. Теория сравнений. Кольцо вычетов. Группа обратимых кольца вычетов. Теорема Вильсона. Функция Эйлера. Теоремы Ферма и Эйлера. Китайская теорема об остатках. Решение систем сравнений. ([1], 2.3., [2], 7–12, [4], 3, [7], IV. 1-3.)

5. Простейшие детерминированные и вероятностные тесты на простоту. Псевдопростые и сильно псевдопростые числа. ([1], 2.3., [3], 4.4., [7], IV. 6.2.)

6. Быстрый алгоритм возведения в степень. Понятие о криптографии с открытыми ключами. Система шифрования RSA. Электроная подпись. ([1], 4.2., [3], 4.1–3., [7], I. 2, IV. 3.)

7. Разложение чисел на множители. Методы Ферма, Диксона и Лежандра ([1], 2.3., [3], 4.7., [5], 4.5.4)

8. Квадратичные вычеты. Свойства символов Лежандра и Якоби. ([2], 21, [4], 5.)

9. Тест Соловея–Штрассена. ([7], IV, упр. 50, 52, 54.)

10. Алгоритм Евклида для многочленов. Вероятностный алгоритм поиска корней сравнения. ([3], 4.2.)

11. Китайская теорема об остатках для многочленов. Алгоритм Бэрлекэмпа. ([5], 4.6.2, [6], 4)

Литература

1. Акритас А. Основы компьютерной алгебры с приложениями. М., Мир, 1994.

2. Бухштаб А.А. Теория чисел. М., Учпедгиз, 1960.

3. Введение в криптографию. М., МЦНМО-ЧеРо, 1998.

4. Виноградов И.М. Основы теории чисел. М.: Наука, 1953.

5. Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М., Мир, 1977.

6. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М., Мир, 1988.

7. Ноден П., Китте К. Алгебраическая алгоритмика. М., Мир, 1999.